IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Group Art Unit:	2137	
Examiner:	Tamara Teslovich	
Inventor:	Herb A. Little	**APPEAL BRIEF**
Serial No.:	09/594,368	
Filed:	6/15/2000	
For:	Public Key Encryption With Digital Signature Scheme	
Atty. Docket:	555255-012130	

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited today with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on March 28, 2006

By Jacqueline M. O'Brien.

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is filed in response to the Final Office Action mailed August 25, 2005, which finally rejected pending claims 1-45 of the instant application. A Notice of Appeal and Request for Pre-Appeal Brief Conference was received by the U.S. Patent Office on November 21, 2005. A Notice of Panel Decision from Pre-Appeal Brief Review was mailed on December 28, 2005.

I. Real Parties In Interest

The real party in interest is Research In Motion Limited as evidenced by an assignment recorded at Reel/Frames 010875/0524-0526.

II. Related Appeals And Interferences

There are no related appeals or interferences to the instant application.

III. Status Of Claims

Claims 1-45 are pending and are finally rejected.

IV. Status Of Amendments

No amendments have been filed subsequent to the final rejection.

V. Summary Of Claimed Subject Matter

In the public-key environment, three are preferably three major processes. First, there is the certification process. A certificate authority creates a certificate that binds a user identity to the public key. A certificate repository provides a database of certificates where the public can access and retrieve the public key information of the participants. In addition, there is a registration authority that acts as an assistant to the certificate authority. In essence, the registration authority is used to validate the binding. The second process is the encryption scheme that essentially converts a plaintext message into a ciphertext message. The third process is the digital signature process, in which a message is digitally singed by a sender using one of a

pair of asymmetric keys. Each of these stages is independent, and each requires a separate degree of processing resources.

The claimed subject matter of independent claims 1, 16 and 31 relate to public key encryption. In particular, independent claims 1, 16 and 31 claim the reuse of an ephemeral key pair from the encryption process in the signature process. Specifically, a plaintext message is encrypted into a ciphertext message. The encrypting of the plaintext into ciphertext also produces an ephemeral key pair. A digital signature may thereafter be signed with the ephemeral key pair.

A. Independent Claim 1

Independent claim 1 claims a public-key encryption process. A first step includes encrypting a plaintext message into a ciphertext message. This encrypting step includes the step of producing an ephemeral key pair. An example implementation of this step is described in the specification at page 9, lines 10-21, and shown in Fig. 4. The next step includes signing a digital signature using the ephemeral key pair. An example implementation of this step is described in the specification at page 9, line 21 - page 10, line 6, and shown in Fig. 4.

B. Independent Claim 16

Independent claim 16 claims a public-key encryption system and comprises two means-plus-function elements. The system includes means for encrypting a plaintext message into a ciphertext message, the means for encrypting producing an ephemeral key pair. This claimed function is described in the specification at page 9, lines 10-21, and shown in Fig. 4. A

corresponding structure for carrying out this claimed function comprises software configured to perform the recited function, hardware configured to perform the recited function, or a combination of software and hardware configured to perform the recited function, as described in the specification at page 10, line 19 - page 11, line 14.

The system also includes means for signing a digital signature using the ephemeral key pair. This claimed function is described in the specification at page 9, line 21 - page 10, line 6, and shown in Fig. 4. A corresponding structure for carrying out this claimed function comprises software configured to perform the recited function, hardware configured to perform the recited function, or a combination of software and hardware configured to perform the recited function, as described in the specification at page 10, line 19 - page 11, line 14, and shown in Fig. 5.

C. Independent Claim 31

Independent claim 31 claims a software program on a computer-readable storage medium that when executed by a processor performs a public-key encryption process. A first step includes encrypting a plaintext message into a ciphertext message. This encrypting step includes the step of producing an ephemeral key pair. An example implementation of this step is described in the specification at page 9, lines 10-21, and shown in Fig. 4. The next step includes signing a digital signature for the ciphertext message using the ephemeral key pair. An example implementation of this step is described in the specification at page 9, line 21 - page 10, line 6, and shown in Fig. 4. The software implementation is further described in the specification at page 10, line 19 - page 11, line 14.

VI. Grounds Of Rejection To Be Reviewed On Appeal

Claims 1-10, 16-25 and 31-40 stand finally rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Pat. No. 5,761,305, issued to Vanstone et al. ("Vanstone"); claims 1, 16 and 31 stand finally rejected under 35 U.S.C. § 102(b) as being anticipated by IBM Technical Bulletin NN9305343 ("IBM Reference"); and claims 11-15, 26-30 and 41-45 stand finally rejected under 35 U.S.C. § 103(a) as being obvious over Vanstone in view of C. Boyd & A. Mathuria, <u>Key Establishment Protocols For Secure Mobile Communications: A Selective Survey,</u> Australian Conference On Information Security And Privacy Proceedings, July 13, 1998 ("Boyd"). These rejections are appealed.

VII. Argument

A. Vanstone Clearly Does Not Anticipate Claims 1, 16 And 31

Claim 1 reads as follows:[1]

1) A public-key encryption process comprising the steps of:
   a) encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair; and
   b) signing a digital signature using the ephemeral key pair.

Claim 1 recites that a plaintext message is encrypted into a ciphertext message and in the encrypting step an ephemeral key pair is produced. That ephemeral key pair is then used in signing a digital signature.

---

[1] Claims 16 and 31 recite similar limitations, and thus the Applicant's remarks with respect to claim 1 apply with

The Examiner maintains that the Vanstone reference discloses the limitations of claim 1. The examiner cites Vanstone at col. 3, lines 1-7 and lines 39-43 for disclosing the limitations of step (a) of claim 1. Vanstone at col. 3, lines 1-7 reads as follows:

> i) a first of said correspondents A selecting a first random integer x and exponentiating a function $f(\alpha)$ including said generator to a power $g(x)$ to provide a first exponentiated function $f(\alpha)^{g(x)}$;
> ii) said first correspondent A generating a first signature s_A from said random integer x and said first exponentiated function $f(\alpha)^{g(x)}$; ...

Vanstone at col. 3, lines 39-43 reads as follows:

> A key 20 is associated with each of cryptographic units 16, 18 to convert plaintext carried between each unit 16, 18 and its respective correspondents 10, 12 into ciphertext carried on the channel 14.

Applicant respectfully disagrees that these passages of Vanstone disclose the limitations of step (a) of claim 1. The protocol described by Vanstone is used to establish a session key with an authenticated correspondent while ensuring that a malicious interloper cannot pretend to be one of the correspondents. This is accomplished by using public keys and signatures of the correspondents when establishing the session key to be used for future communications between them. Thus, steps (i) and (ii) of Vanstone are not used to encrypt a plaintext message into a ciphertext message as required by claim 1. Instead, the introductory sentence in this passage in Vanstone states that these steps (i) and (ii) are used in "a method of establishing a <u>session key</u> between a pair of correspondents A, B to permit exchange of information therebetween." (Vanstone, col. 2, ll. 62-64). "The session key is <u>subsequently</u> used to achieve some

---

equal force to claims 16 and 31.

cryptographic goal, such as privacy." (Vanstone, col. 1, ll. 32-33). Vanstone elaborates on the use of this established session key stating that "a message generated by correspondent A, 10, is encrypted by the unit 16 with the key 20 and transmitted as ciphertext over channel 14 to the unit 18. The key 20 operates upon the ciphertext in the unit 18 to generate a plaintext message for the correspondent B, 12." (Vanstone, col. 3, ll. 44-46). Vanstone stresses that "in order for the system shown in FIG. 1 to operate it is necessary for the keys 20 to be identical and therefore a key agreement protocol is established that allows the transfer of information in a public manner to establish the identical keys." (Vanstone, col. 3, ll. 52-56).

More to the point, Vanstone generates an asymmetric key pair to generate a digital signature (Vanstone, col. 3, ll. 1-17, steps i-iv) to authenticate the correspondents involved in the key establishment process, and then generates a separate symmetric session key to encrypt a plaintext message into a ciphertext message in a later encryption step (Vanstone, col. 3, ll. 21-24, step v). Vanstone thus cannot anticipate "encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair" because:

1) the encrypting of plaintext into ciphertext in Vanstone does not produce the claimed ephemeral key pair that is used in signing the digital signature - the encryption in Vanstone occurs after and separate from the production of any key pair and thus does not fall within the plain language of the claim; and

2) the establishing of the session key does not meet the claim language of "the encrypting step includes the step of producing an ephemeral key pair" because the asymmetric key pairs described in Vanstone at col. 3, ll. 1-19 are

> generated <u>before</u> the encrypting step and <u>in order to establish a symmetric session key</u> for later use when encrypting messages.

See, e.g., Vanstone, Abstract; col. 2, ln. 61 - col. 3, ln. 24; col. 4, ll. 19-36; col. 4, ln. 60 - col. 5, ln. 4; col. 5, ln. 25 - col. 6, ln. 10.

In summary, the Examiner admits that claim 1 teaches that an encryption step is followed by a signing step:

> Claim 1 discloses the step of encrypting, including producing an ephemeral key <u>followed by the signing step</u> wherein the ephemeral key pair is then used to sign a digital signature.

Final Office Action, pg. 2 (emphasis added). Thereafter, however, the Examiner relies on Vanstone, which teaches the use of digital signatures to establish a key pair <u>that is later used for the encrypting step</u>, to reject claim 1. This rejection is clearly improper.

Vanstone therefore fails to anticipate claims 1, 16, and 31. Additionally, because the rejections of all dependent claims are predicated on the incorrect rejections of claim 1, 16 and 31, the Applicant respectfully requests that all the 35 U.S.C. §§ 102 and 103 rejections of claims 1-45 be withdrawn.

II. The IBM Reference Clearly Does Not Anticipate Claims 1, 16 And 31

The Examiner <u>admits</u> that the term "ephemeral key pair" is not mentioned in the IBM Reference, but nevertheless concludes that the IBM Reference anticipates claims 1, 16 and 31 because the reference refers to the RSA algorithm:

> Note that although the phrase "ephemeral key pair" does not appear in the above mentioned passage, IBM utilizes the RSA algorithm, which is known to

> utilize session keys, which are by definition ephemeral keys. For example, SSL has been using these ephemeral RSA keys publicly as far back as 1993.[2]

Final Office Action, pg. 11. This rejection is improper because it fails to show how all the limitations of claims 1, 16 and 31 are disclosed, and because the session key of the RSA algorithm is not the claimed key pair that is used to sign a digital signature.

First, the rejection is conclusory and does not show how the IBM Reference discloses "the encrypting step includes the step of producing an ephemeral key pair." The reference does not specifically teach that an ephemeral key pair is created from an encrypting step, and, as the Examiner admits, this limitation is not even addressed in the IBM reference.

Second, the rejection also does not show how the IBM reference discloses "signing a digital signature using the ephemeral key pair." The Examiner appears to be confusing a session key with a key pair. A "session key" is a single symmetric key for encrypting text. It is not a key pair that is used to sign a digital signature. Vanstone at col. 3, ll. 52-59 makes clear that the session key is a single key and not a key pair ("in order for the system of Fig. 1 to operate it is necessary for the keys 20 to be identical..."). The Examiner simply ignores the claim language that recites a "key pair" which connotes to one of ordinary skill in the art a pair of asymmetric keys. See specification, pg. 9, ll. 13-21. A session key is a single key shared between two or more parties. It is not a "key pair" according to the plain and ordinary meaning known to one of ordinary skill in the art and as used in the specification and the claims.

---

[2] The passage cited by the Examiner in the Final Office Action is not accurately quoted. Sentences are either paraphrases or quoted from several paragraphs beginning on page 1, line 39 - page 2, line 14. Additionally, this particular rejection, which is under 35 U.S.C. § 102(b), is included in the section of rejections listed under 35 U.S.C. § 103(a). However, the rejection is clearly directed to anticipation, not obviousness. Accordingly, the Applicant responds to this rejection as a 35 U.S.C. § 102(b) rejection.

Thus the IBM Reference has not been shown to anticipate all of the claimed limitations of claims 1, 16 or 31. Because the Examiner has failed to show how claims 1, 16 or 31 are anticipated, these claims, and all claims depending therefrom, are in condition for allowance.

VIII. Claims Appendix

A claims appendix containing a copy of the claims subject to this appeal is attached.

IX. Evidence Appendix

No evidence is being submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132, nor is there any other evidence entered by the Examiner or relied upon by the Applicant. An evidence appendix indicating "None" is attached.

X. Related Proceedings Appendix

There are no related proceedings. A related proceedings appendix indicating "None" is attached.

Respectfully submitted,

Date: 2/28/6

By: ______________________

Paul E. Franz, Reg. No. 45,910
Jones Day
North Point
901 Lakeside Ave.
Cleveland, Ohio 44114
(216) 586-1162

CLAIMS APPENDIX

1. (ORIGINAL) A public-key encryption process comprising the steps of:

c) encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair; and

d) signing a digital signature using the ephemeral key pair.

2. (ORIGINAL) A public-key encryption process according to claim 1, wherein the encrypting step uses an El Gamal encryption scheme.

3. (PREVIOUSLY PRESENTED) A public-key encryption process according to claim 1, wherein the step of signing a digital signature comprises generating the digital signature using a Nyberg-Rueppel digital signature scheme;

wherein the step of generating the digital signature includes hashing the plaintext message.

4. (ORIGINAL) A public-key encryption process according to claim 1, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key x and calculating an encryption ephemeral public key $X = xG$, where G is a generator.

5. (ORIGINAL) A public-key encryption process according to claim 1, for encrypting messages for communication between a sender and a receiver, the process further

comprising the steps of,

at the sender,

a) generating a sender private key a; and

b) calculating a sender public key $A = aG$, where G is a generator,

and at the receiver,

a) generating a receiver private key b; and

b) calculating a receiver public key $B = bG$,

wherein the sender obtains an authentic copy of the receiver public key B and the receiver obtains an authentic copy of the sender public key A.

6. (ORIGINAL) A public-key encryption process according to claim 5, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key x and calculating an encryption ephemeral public key $X = xG$.

7. (ORIGINAL) A public-key encryption process according to claim 6, further comprising the steps of, at the sender, generating a secret key $K = xB$ and encrypting a plaintext message using the secret key K to generate a ciphertext message.

8. (ORIGINAL) A public-key encryption process according to claim 7, further comprising the steps of, at the sender, using the encryption private key x as a signature ephemeral private key and using the encryption ephemeral public key X as a signature ephemeral public key to generate a digital signature.

9. (ORIGINAL) A public-key encryption process according to claim 8, wherein the digital signature comprises a first value r and a second value s, the process further comprising the step of, at the sender, transmitting the encryption ephemeral public key X, the ciphertext message and the second value s of the digital signature to the receiver.

10. (ORIGINAL) A public-key encryption process according to claim 9, further comprising the steps of, at the receiver, generating the secret key $K = bX = bxG = xbG = xB$, decrypting the transmitted ciphertext message using the generated secret key K, calculating the first value r of the digital signature using the decrypted message and the transmitted encryption ephemeral public key X and validating the digital signature based on the calculated first value r and the transmitted second value s.

11. (PREVIOUSLY PRESENTED) A public-key encryption process according to claim 1, implemented in a wireless communication system;

    wherein at least a two stage public-key encryption process is used;

    wherein the first stage includes key establishment and the second stage includes encryption/decryption;

    wherein said steps (a) and (b) are performed during the second stage of encryption.

12. (ORIGINAL) A public-key encryption process according to claim 1, implemented in a wireless hand-held communication device.

13. (ORIGINAL) A public-key encryption process according to claim 1, implemented in a personal digital assistant.

14. (ORIGINAL) A public-key encryption process according to claim 1, implemented in a cellular phone.

15. (ORIGINAL) A public-key encryption process according to claim 1, implemented in a two-way pager.

16. (ORIGINAL) A public-key encryption system comprising:

a) means for encrypting a plaintext message into a ciphertext message, the means for encrypting producing an ephemeral key pair; and

b) means for signing a digital signature using the ephemeral key pair.

17. (ORIGINAL) A public-key encryption system according to claim 16, wherein the means for encrypting employs an E1 Gamal encryption scheme.

18. (ORIGINAL) A public-key encryption system according to claim 16, wherein the means for signing a digital signature generates the digital signature using a Nyberg-Rueppel digital signature scheme.

19. (ORIGINAL) A public-key encryption system according to claim 16, wherein the means for encrypting produces the ephemeral key pair by generating an encryption ephemeral private key x and calculating an encryption ephemeral public key $X = xG$ where G is a generator.

20. (ORIGINAL) A public-key encryption system according to claim 16, for encrypting messages for communication between a sender and a receiver, the system further comprising, at the sender,

a) means for generating a sender private key a; and

b) means for calculating a sender public key $A = aG$, where G is a generator, and at the receiver,

a) means for generating a receiver private key b; and

b) means for calculating a receiver public key $B = bG$,

wherein the sender obtains an authentic copy of the receiver public key B and the receiver obtains authentic copy of the sender public key A.

21. (ORIGINAL) A public-key encryption system according to claim 20, wherein the means for encrypting produces the ephemeral key pair by generating an encryption ephemeral private key x and calculating an encryption ephemeral public key $X = xG$.

22. (ORIGINAL) A public-key encryption system according to claim 21, wherein the means for encrypting generates a secret key $K = xB$ and uses the secret key K to encrypt a

plaintext message and thereby generate a ciphertext message.

23. (ORIGINAL) A public-key encryption system according to claim 22, wherein the means for signing uses the encryption private key x as a signature ephemeral private key and uses the encryption ephemeral public key X as a signature ephemeral public key to generate a digital signature.

24. (ORIGINAL) A public-key encryption system according to claim 23, wherein the digital signature comprises a first value r and a second value s, the system further comprising, at the sender, means for transmitting the encryption ephemeral public key X, the ciphertext message and only the second value s of the digital signature to the receiver.

25. (ORIGINAL) A public-key encryption system according to claim 24, further comprising, at the receiver, means for decrypting a ciphertext message and means for validating a digital signature, wherein the means for decrypting generates the secret key K = bX and decrypts the transmitted ciphertext message using the generated secret key K, and the means for validating calculates the first value r of the digital signature using the decrypted message and the transmitted encryption ephemeral public key X and validates the digital signature based on the calculated first value r and the transmitted second value s.

26. (ORIGINAL) A public-key encryption system according to claim 16, implemented in a wireless communication system.

27. (ORIGINAL) A public-key encryption system according to claim 16, implemented in a wireless hand-held communication device.

28. (ORIGINAL) A public-key encryption system according to claim 16, implemented in a personal digital assistant.

29. (ORIGINAL) A public-key encryption system according to claim 16, implemented in a cellular phone.

30. (ORIGINAL) A public-key encryption system according to claim 16, implemented in a two-way pager.

31. (ORIGINAL) A software program on a computer-readable storage medium, which when executed by a processor performs a public-key encryption process comprising the steps of:

a) encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair; and

b) signing a digital signature for the ciphertext message using the ephemeral key.

32. (ORIGINAL) A software program according to claim 31, wherein the encrypting step uses an El Gamal encryption scheme.

33. (ORIGINAL) A software program according to claim 31, wherein the step of signing a digital signature comprises generating the digital signature using a Nyberg-Rueppel digital signature scheme.

34. (ORIGINAL) A software program according to claim 31, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key x and calculating an encryption ephemeral public key $X = xG$, where G is a generator.

35. (ORIGINAL) A software program according to claim 31, for encrypting messages for communication between a sender and a receiver, the software program performing the further steps of, at the sender,

a) generating a sender private key a; and

b) calculating a sender public key $A = aG$, where G is a generator,

and at the receiver,

a) generating a receiver private key b; and

b) calculating a receiver public key $B = bG$,

wherein the sender obtains an authentic copy of the receiver public key B and the receiver obtains an authentic copy of the sender public key A.

36. (ORIGINAL) A software program according to claim 35, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private

key x and calculating an encryption ephemeral public key $X = xG$.

37. (ORIGINAL) A software program according to claim 36, wherein the software program performs the further steps of, at the sender, generating a secret key $K = xB$ and encrypting a plaintext message using the secret key K to generate a ciphertext message.

38. (ORIGINAL) A software program according to claim 37, wherein the software program performs the further steps of, at the sender, using the encryption private key x as a signature ephemeral private key and using the encryption ephemeral public key X as a signature ephemeral public key to generate a digital signature.

39. (ORIGINAL) A software program according to claim 38, wherein the digital signature comprises a first value r and a second value s, the software program performing the further step of, at the sender, transmitting the encryption ephemeral public key X, the ciphertext message and the second value s of the digital signature to the receiver.

40. (ORIGINAL) A software program according to claim 39, the software program performing the steps of, at the receiver, generating the secret key $K = bX = bxG = xbG = xB$, decrypting the transmitted ciphertext message using the generated secret key K, calculating the first value r of the digital signature using the decrypted message and the transmitted encryption ephemeral public key X and validating the digital signature based on the calculated first value r and the transmitted second value s.

41. (ORIGINAL) A software program according to claim 31, installed in a wireless communication system.

42. (ORIGINAL) A software program according to claim 31, installed in a wireless hand-held communication device.

43. (ORIGINAL) A software program according to claim 31, installed in a personal digital assistant.

44. (ORIGINAL) A software program according to claim 31, installed in a cellular phone.

45. (ORIGINAL) A software program according to claim 31, installed in a two-way pager.

EVIDENCE APPENDIX

NONE

(No evidence is being submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132, nor is there any other evidence entered by the Examiner or relied upon by the Applicant)

RELATED PROCEEDINGS APPENDIX

NONE

(There are no related proceedings)